Notice of Allowability	Application No.	Applicant(s)	
	09/315,628	JAKOBSSON, BJORN MARKUS	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *9/24/04*.

2. ☒ The allowed claim(s) is/are *1-27*.

3. ☒ The drawings filed on *15 April 2004* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. The response of 9/24/04 was received and considered.

2. Claims 1-27 are allowed.

3. In light of applicant's amendments to the claims, the rejections of claims 1-10, 17, 22-23, 25 & 27 under 35 U.S.C. §101, and claim 17 under 35 U.S.C. §112 ¶2 are withdrawn.

Allowable Subject Matter

4. Claims 1-27 are allowed.

5. The following is an examiner's statement of reasons for allowance:

Regarding claims 1, 11, 22, 25, 26 & 27, the prior art relied upon fails to teach or suggest generating information representative of first and second proofs both performed by the same prover based on an operation associated with a cryptographic protocol, wherein the first proof is a proof that the operation has been correctly performed and the second proof is a proof that the first proof has been correctly performed, wherein the information representative of the first and second proofs is used, at least in part, to determine if the operation associated with the cryptographic protocol is valid. The prior art of record shows a first and second proof, wherein the first proof is a proof that the operation has been correctly performed ad the second proof is a proof that the first proof has been correctly performed (Menezes, as cited in the previous Office Action), but fails to teach both proofs performed by the same prover.

Regarding claims 23 & 24, the prior art relied upon fails to teach or suggest a transformation protocol which produces a pair (G,Y) wherein G is a generator and Y is a public key such that $X = \log_G Y$ can only be computed if $\log_g y = \log_m s$ and generates a digital

signature using (G, Y). Chaum et al., in "Undeniable Signatures" discloses a generator, g, a private key x and it's corresponding public key y (p. 213). Page 1 of applicant's specification states that Chaum et al. "attempt to determine whether a given quadruple (g, y, m, s) satisfies the relation $\log_g y = \log_m s$ in the context of verifying the validity of undeniable signatures". Chaum's $\log_g y = \log_m s$ verifies if the 'private key' x corresponding to the public key $y = g^x$ is the same x used in creation of a digital signature $s = m^x$. However, none of the references teach or suggest that a generator $X = \log_G Y$ can only be computed if $\log_g y = \log_m s$.

Regarding specifically claims 11, 24 & 26, in the limitation "a processor associated ... and operative", the word "operative" is understood to mean "programmed", rather than simply "capable of performing the operations".

6. Claims 2-10 are allowable based on their dependence upon claim 1.

7. Claims 12-21 are allowable based on their dependence upon claim 11.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
January 11, 2005

5/16/05

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100